1. A method for initializing secure communications between a first device and a second device, said first and second devices each having a public key of a Certificate Authority and a device certificate, said device certificate having a unique hardware identifier associated with said respective device, and a public key associated with said respective device, said method comprising the steps of:

establishing a session between said first device and said second device;

negotiating two-way session encryption and mutual authentication requirements between said first and said second device;

exchanging device certificates of said first device and said second device;

cryptographically verifying the received certificate using the public key of said Certificate Authority;

exchanging challenges created by each of said first and second devices;

responding to said respective challenges by signing said received challenge, using the receiving device's private key, said private keys residing in the respective protected storage in each said device;

returning said signed challenges;

cryptographically verifying that said received challenge signature is of the challenge previously sent by said receiving device;

establishing a key agreement between said first and said second devices; and,

establishing secure communications if all of said prior verifying steps succeed.

2. A method as claimed in claim 1 wherein said first established session is non-secure.

3. A method as claimed in claim 1 wherein said first established session is an authenticated connection.

4. A method as claimed in claim 1 wherein said first established session is an encrypted connection.

5. A method as claimed in claim 1 wherein said unique hardware identifier is a machine (MAC) address for said associated device.

6. A method as claimed in claim 1 wherein said protected storage is a write-only storage with the ability to perform computations involving previously-written data.

7. A method as claimed in claim 1 wherein said protected storage is read-write storage wherein the read capacity of said storage is accessible only by means of a shared secret.

8. A method as claimed in claim 1 wherein said public key of a Certificate Authority is a public key of a root Certificate Authority.

9. A program for initializing secure communications between a first device and a second device, said first and second devices each having a public key of a Certificate Authority and a device certificate, said device certificate having a unique hardware identifier associated with said respective device, and a public key associated with said respective device, said program code comprising:

computer program code means for establishing a session between said first device and said second device;

computer program code means for negotiating two-way session encryption and mutual authentication requirements between said first and said second device;

computer program code means for exchanging device certificates of said first device and said second device;

computer program code means for cryptographically verifying the received certificate using the public key of said Certificate Authority;

computer program code means for exchanging challenges created by each of said first and second devices;

computer program code means for responding to said respective challenges by signing said received challenge, using the receiving device's private key, said private keys residing in the respective protected storage in each said device;

computer program code means for returning said signed challenges;

computer program code means for cryptographically verifying that said received challenge signature is of the challenge previously sent by said receiving device;

computer program code means for establishing a key agreement between said first and said second devices; and,

computer program code means for establishing secure communications if all of said prior verifying steps succeed.

10. A program as claimed in claim 9 wherein said first established session is non-secure.

11. A program as claimed in claim 9 wherein said first established session is an authenticated connection.

12. A program as claimed in claim 9 wherein said first established session is an encrypted connection.

13. A program as claimed in claim 9 wherein said unique hardware identifier is a machine (MAC) address for said associated device.

14. A program as claimed in claim 9 wherein said protected storage is a write-only storage with the ability to perform computations involving previously-written data.

15. A program as claimed in claim 9 wherein said protected storage is read-write storage wherein the read capacity of said storage is accessible only by means of a shared secret.

16. A program as claimed in claim 9 wherein said public key of a Certificate Authority is a public key of a root Certificate Authority.

17. A system for initializing secure communications between a first device and a second device, said first and second devices each having a public key of a Certificate Authority and a device certificate, said device certificate having a unique hardware identifier associated with said respective device, and a public key associated with said respective device, said system comprising:

a communications mechanism for establishing a session between said first device and said second device, negotiating two-way session encryption and mutual authentication requirements between said first and said second device, and exchanging device certificates of said first device and said second device;

a verifier for cryptographically verifying the received certificate using the public key of said Certificate Authority;

a negotiation mechanism for exchanging challenges created by each of said first and second devices, responding to said respective challenges by signing said received challenge, using the receiving device's private key, said private keys residing in the respective protected storage in each said device, returning said signed challenges,

cryptographically verifying that said received challenge signature is of the challenge previously sent by said receiving device,establishing a key agreement between said first and said second devices; and, establishing secure communications if all of said prior verifying steps succeed.

18. A system as claimed in claim 17 wherein said first established session is non-secure.

19. A system as claimed in claim 17 wherein said first established session is an authenticated connection.

20. A system as claimed in claim 17 wherein said first established session is an encrypted connection.

21. A system as claimed in claim 17 wherein said unique hardware identifier is a machine (MAC) address for said associated device.

22. A system as claimed in claim 17 wherein said protected storage is a write-only storage with the ability to perform computations involving previously-written data.

23. A system as claimed in claim 17 wherein said protected storage is read-write storage wherein the read capacity of said storage is accessible only by means of a shared secret.

24. A system as claimed in claim 17 wherein said public key of a Certificate Authority is a public key of a root Certificate Authority.